DIOPHANTINE DEFINABILITY OF INFINITE DISCRETE NON-ARCHIMEDEAN SETS AND DIOPHANTINE MODELS OVER LARGE SUBRINGS OF NUMBER FIELDS

BJORN POONEN AND ALEXANDRA SHLAPENTOKH

Abstract. We prove that infinite $\mathfrak{p}$-adically discrete sets have Diophantine definitions in large subrings of some number fields. First, if K is a totally real number field or a totally complex degree-2 extension of a totally real number field, then there exists a prime $\mathfrak{p}$ of K and a set of K-primes $\mathcal{S}$ of density arbitrarily close to 1 such that there is an infinite $\mathfrak{p}$-adically discrete set that is Diophantine over the ring $\mathcal{O}_{K,\mathcal{S}}$ of $\mathcal{S}$-integers in K. Second, if K is a number field over which there exists an elliptic curve of rank 1, then there exists a set of K-primes $\mathcal{S}$ of density 1 and an infinite Diophantine subset of $\mathcal{O}_{K,\mathcal{S}}$ that is v-adically discrete for every place v of K. Third, if K is a number field over which there exists an elliptic curve of rank 1, then there exists a set of K-primes $\mathcal{S}$ of density 1 such that there exists a Diophantine model of $\mathbb{Z}$ over $\mathcal{O}_{K,\mathcal{S}}$. This line of research is motivated by a question of Mazur concerning the distribution of rational points on varieties in a non-archimedean topology and questions concerning extensions of Hilbert's Tenth Problem to subrings of number fields.

1. Introduction

Matijasevič (following work of Davis, Putnam, and Robinson) proved that Hilbert's Tenth Problem could not be solved: that is, there does not exist an algorithm, that given an arbitrary multivariable polynomial equation $f(x_1, \dots, x_n) = 0$ with coefficients in $\mathbb{Z}$, decides whether or not a solution in $\mathbb{Z}^n$ exists. It is not known whether an analogous algorithm exists, however, if in the problem one replaces $\mathbb{Z}$ by $\mathbb{Q}$ in both places. One natural approach to proving a negative answer for $\mathbb{Q}$ is to show that $\mathbb{Z}$ admits a Diophantine definition over $\mathbb{Q}$, or more generally that there is a Diophantine model of the ring $\mathbb{Z}$ over $\mathbb{Q}$; the meaning of these statements is given in Definitions 1.1 and 1.3 below. (See [DLPVG00] for an introduction to the subject.)

Definition 1.1. Let R be a (commutative) ring. Suppose $A \subseteq R^k$ for some $k \in \mathbb{N}$. Then we say that A has a *Diophantine definition over* R if there exists a polynomial

$$f(t_1, \dots, t_k, x_1, \dots, x_n) \in R[t_1, \dots, t_k, , x_1, \dots, x_n]$$

such that for any $(t_1, \dots, t_k) \in R^k$,

$$(t_1, \dots, t_k) \in A \iff \exists x_1, \dots, x_n \in R,\ f(t_1, \dots, t_k, x_1, ..., x_n) = 0.$$

Date: August 19, 2004.

2000 *Mathematics Subject Classification.* Primary 11U05; Secondary 11G05.

Key words and phrases. Hilbert's Tenth Problem, elliptic curve, Mazur's Conjecture, Diophantine definition, norm equation.

B.P. was partially supported by a Packard Fellowship and by NSF grants DMS-9801104 and DMS-0301280. A.S. was partially supported by NSF grants DMS-9988620 and DMS-0354907, and by ECU Faculty Senate Summer 2003 Grant.

In this case we also say that A is a *Diophantine subset* of R^k, or that A is *Diophantine over R*.

Remark 1.2. Suppose that R is a domain whose quotient field is not algebraically closed. Then

(a) Relaxing Definition 1.1 to allow an arbitrary finite conjunction of equations in place of the single equation on the right hand side does not enlarge the collection of Diophantine sets.

(b) Unions and intersections of Diophantine sets are Diophantine.

See the introduction in [Phe94] for details.

Definition 1.3. A *Diophantine model of $\mathbb{Z}$ over a ring R* is a Diophantine subset $A \subseteq R^k$ for some k together with a bijection $\phi\colon \mathbb{Z} \to A$ such that the graphs of addition and multiplication (subsets of $\mathbb{Z}^3$) correspond under ϕ to Diophantine subsets of $A^3 \subseteq R^{3k}$.

Mazur formulated a conjecture that would imply that a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$ does not exist, and later in [CZ00] it was found that his conjecture also ruled out the existence of a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$. One form of Mazur's conjecture was that for a variety X over $\mathbb{Q}$, the closure of $X(\mathbb{Q})$ in the topological space $X(\mathbb{R})$ should have at most finitely many connected components. See [Maz92], [Maz94], [Maz95], [Maz98], [CTSSD97], [CZ00], [Poo03], and [Shl03] for more about the conjecture and its consequences.

Mazur also formulated an analogue applying to both archimedean and nonarchimedean completions of arbitrary number fields. Specifically, on page 257 of [Maz98] he asked:

Question 1.4. Let V be any variety defined over a number field K. Let $\mathcal{S}$ be a finite set of places of K, and consider $K_{\mathcal{S}} = \prod_{v\in\mathcal{S}} K_v$ viewed as locally compact topological ring. Let $V(K_{\mathcal{S}})$ denote the topological space of $K_{\mathcal{S}}$-rational points. For every point $p \in V(K_{\mathcal{S}})$ define $W(p) \subset V$ to be the subvariety defined over K that is the intersection of Zariski closures of the subsets $V(K) \cap U$, where U ranges through all open neighborhoods of p in $V(K_{\mathcal{S}})$. As p ranges through the points of $V(K_{\mathcal{S}})$, are there only a finite number of distinct subvarieties $W(p)$?

In Question 1.4, it does not matter whether we require V to be irreducible. (We will not.)

Proposition 1.5. *Fix a number field K and a place $\mathfrak{p}$. If Question 1.4 has a positive answer for K and $\mathcal{S} := \{\mathfrak{p}\}$, then there does not exist an infinite, $\mathfrak{p}$-adically discrete, Diophantine subset of K.*

Proof. Suppose there exists a subset A of K that is infinite, $\mathfrak{p}$-adically discrete, and Diophantine over K. The Diophantine definition of A corresponds to an affine algebraic set V such that the projection $\pi : V \to \mathbb{A}^1$ onto the first coordinate satisfies $\pi(V(K)) = A$.

Suppose $a \in A$. Since A is $\mathfrak{p}$-adically discrete, there exists an open neighborhood N of a in $K_{\mathfrak{p}}$ such that $A \cap N = \{a\}$. Pick $p \in V(K)$ with $\pi(p) = a$. Then $U := \pi^{-1}(N)$ is an open neighborhood of p, and π maps $V(K) \cap U$ into $A \cap N = \{a\}$, so $W(p) \subseteq \pi^{-1}(a)$.

By choosing one p above each $a \in A$, we get infinitely many disjoint subvarieties $W(p)$, contradicting the positive answer to Question 1.4. □

In view of the proposition above, constructing a Diophantine definition of an infinite discrete $\mathfrak{p}$-adic set over a number field K would be one way to answer Question 1.4 (negatively) for K. Unfortunately, at the moment such a construction seems out of reach. Thus instead we consider analogues in which K is replaced by some of its large integrally closed subrings.

Definition 1.6. If K is a number field, let $\mathcal{P}_K$ be the set of finite primes of K. For $\mathcal{S} \subseteq \mathcal{P}_K$, define the *ring of $\mathcal{S}$-integers*

$$\mathcal{O}_{K,\mathcal{S}} = \{\, x \in K \mid \operatorname{ord}_{\mathfrak{p}} x \geq 0 \text{ for all } \mathfrak{p} \notin \mathcal{S} \,\}.$$

(Elsewhere the term $\mathcal{S}$-integers often presupposes that $\mathcal{S}$ is finite, but we will use this term for infinite $\mathcal{S}$ also.)

If $\mathcal{S} = \emptyset$, then $\mathcal{O}_{K,\mathcal{S}}$ equals the ring $\mathcal{O}_K$ of algebraic integers of K. If $\mathcal{S} = \mathcal{P}_K$, then $\mathcal{O}_{K,\mathcal{S}} = K$. In general, $\mathcal{O}_{K,\mathcal{S}}$ lies somewhere between $\mathcal{O}_K$ and K, and the density of $\mathcal{S}$ (if it exists) may be used as a measure of the "size" of $\mathcal{O}_{K,\mathcal{S}}$. Throughout this paper, "density" means *natural density*, which is defined as follows.

Definition 1.7. Let $\mathcal{S} \subseteq \mathcal{P}_K$. The *density* of $\mathcal{S}$ is defined to be the limit

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in \mathcal{S} : N\mathfrak{p} \leq X\}}{\#\{\text{all } \mathfrak{p} : N\mathfrak{p} \leq X\}}$$

if it exists. If the density of $\mathcal{S}$ does not exist, we can replace the limit in Definition 1.7 by lim sup or lim inf and hence define the upper or lower densities of $\mathcal{S}$. (See [Lan94, VIII, §4] for more about density.)

The study of Diophantine definability and the archimedean conjecture of Mazur over rings of $\mathcal{S}$-integers has produced Diophantine definitions of $\mathbb{Z}$ and discrete archimedean sets over large subrings of some number fields (see [Shl97], [Shl00a], [Shl02], [Shl] and [Shl03]). Recently in [Poo03], the first author constructed an infinite discrete Diophantine set (in the archimedean topology) and a Diophantine model of $\mathbb{Z}$ over a subring of $\mathbb{Q}$ corresponding to a set of primes of density 1. Thus he showed that the analogue of Hilbert's Tenth Problem is undecidable over such a ring.

In this paper we consider Diophantine definability of infinite discrete $\mathfrak{p}$-adic sets over some rings of $\mathcal{S}$-integers. Our results will come from two sources: norm equations (as in [Shl03]) and elliptic curves (as in [Poo03]). Our main results are stated below. When we say that a subset of $\mathcal{O}_{K,\mathcal{S}}$ is Diophantine, we mean that it is Diophantine *over* $\mathcal{O}_{K,\mathcal{S}}$. A subset $\mathcal{S}$ of $\mathcal{P}_K$ is *recursive* if there exists an algorithm that takes as input an element of K (given by its coordinates with respect to some fixed $\mathbb{Q}$-basis) and decides whether it belongs to $\mathcal{O}_{K,\mathcal{S}}$.

Theorem 1.8. *Let K be a totally real number field or a totally complex degree-2 extension of a totally real number field. Let $\mathfrak{p}$ be any prime of K. Then for any $\varepsilon > 0$ there exists a recursive set of K-primes $\mathcal{S}$ containing $\mathfrak{p}$ of density $> 1 - \varepsilon$ such that there exists an infinite Diophantine subset of $\mathcal{O}_{K,\mathcal{S}}$ that is discrete and closed when viewed as a subset of the completion $K_{\mathfrak{p}}$.*

Theorem 1.9. *Let K be any number field for which there exists an elliptic curve E such that* $\operatorname{rank} E(K) = 1$. *Then*

(1) *There exist recursive subsets $\mathcal{T}_1, \mathcal{T}_2 \subseteq \mathcal{P}_K$ of density 0 such that for any $\mathcal{S}$ with $\mathcal{T}_1 \subseteq \mathcal{S} \subseteq \mathcal{P}_K - \mathcal{T}_2$, there exists an infinite Diophantine subset A of $\mathcal{O}_{K,\mathcal{S}}$ such that for all places v of K, the set A is discrete when viewed as a subset of the completion K_v.*

(2) *There exist recursive subsets $\mathcal{T}_1', \mathcal{T}_2' \subseteq \mathcal{P}_K$ of density 0 such that for any $\mathcal{S}$ with $\mathcal{T}_1' \subseteq \mathcal{S} \subseteq \mathcal{P}_K - \mathcal{T}_2'$, there exists a Diophantine model of the ring $\mathbb{Z}$ over $\mathcal{O}_{K,\mathcal{S}}$.*

2. Using Norm Equations

In this section we use norm equations to construct infinite Diophantine $\mathfrak{p}$-adically discrete sets, in order to prove Theorem 1.8.

2.1. **Preliminary results.**

Proposition 2.1. *Let K be a number field and let $\mathcal{S} \subseteq \mathcal{P}_K$. The $\mathcal{O}_{K,\mathcal{S}} - \{0\}$ is Diophantine over $\mathcal{O}_{K,\mathcal{S}}$.*

Proof. See Proposition 2.6 on page 113 of [Shl00b]. (Note: there is a typo in the statement in [Shl00b]: the last K should be $\mathcal{O}_{K,W}$.) □

The importance of Proposition 2.1 is that equations with variables intended to range over K can now be interpreted in the arithmetic of $\mathcal{O}_{K,\mathcal{S}}$, since elements of K can be represented as fractions of elements of $\mathcal{O}_{K,\mathcal{S}}$ with nonzero denominator.

Proposition 2.2. *Let K be a number field, and let $\mathfrak{p} \in \mathcal{P}_K$. Then the discrete valuation ring $\mathcal{O}_{K,\mathcal{P}_K - \{\mathfrak{p}\}} = \{\, x \in K : \operatorname{ord}_{\mathfrak{p}} x \geq 0 \,\}$ is Diophantine over K.*

Proof. See Lemma 3.22 in [Shl94]. □

Corollary 2.3. *Let K be a number field, and let $\mathfrak{p} \in \mathcal{P}_K$. Then the sets $\{\, x \in K : \operatorname{ord}_{\mathfrak{p}} x > 0 \,\}$, $\{\, (x,y) \in K^2 : \operatorname{ord}_{\mathfrak{p}} x \geq \operatorname{ord}_{\mathfrak{p}} y \,\}$, and $\{\, (x,y) \in K^2 : \operatorname{ord}_{\mathfrak{p}} x = \operatorname{ord}_{\mathfrak{p}} y \,\}$ are Diophantine over K.*

Proof. Fix $a \in K$ with $\operatorname{ord}_{\mathfrak{p}} a = 1$. Then

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}} x > 0 \quad &\iff \quad \operatorname{ord}_{\mathfrak{p}}(x/a) \geq 0, \\ \operatorname{ord}_{\mathfrak{p}} x \geq \operatorname{ord}_{\mathfrak{p}} y \quad &\iff \quad (\exists r)(x = ry \quad \text{and} \quad \operatorname{ord}_{\mathfrak{p}} r \geq 0), \\ \operatorname{ord}_{\mathfrak{p}} x = \operatorname{ord}_{\mathfrak{p}} y \quad &\iff \quad (\operatorname{ord}_{\mathfrak{p}} x \geq \operatorname{ord}_{\mathfrak{p}} y) \text{ and } (\operatorname{ord}_{\mathfrak{p}} y \geq \operatorname{ord}_{\mathfrak{p}} x). \end{aligned}$$

□

Propositions 2.1 and 2.2 together imply the following generalization of Proposition 2.2 (cf. Theorem 4.4 in [Shl94]):

Proposition 2.4. *Let K be a number field. If $\mathcal{S} \subseteq \mathcal{S}' \subseteq \mathcal{P}_K$ and $\mathcal{S}' - \mathcal{S}$ is finite, then $\mathcal{O}_{K,\mathcal{S}}$ is Diophantine over $\mathcal{O}_{K,\mathcal{S}'}$.*

Lemma 2.5. *Let F be a number field. Let $\{\omega_1, \ldots, \omega_s\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_F$. Let $a_1, \ldots, a_s \in \mathbb{Q}$, and let $x = \sum_{i=1}^{s} a_i \omega_i$. Let p be a prime of $\mathbb{Q}$ that does not ramify in F. Then*

$$\min_i \operatorname{ord}_p a_i = \min_{\mathfrak{P}} \operatorname{ord}_{\mathfrak{P}} x,$$

where $\mathfrak{P}$ ranges over F-primes above p.

Proof. Since p is unramified in F, the ideal $p\mathcal{O}_F$ factors as the product of the $\mathfrak{P}$. Thus we have an equality $p^m \mathcal{O}_F = \prod_{\mathfrak{P}} \mathfrak{P}^m$ for any $m \in \mathbb{Z}$. The two minimums in the statement equal the largest m for which x belongs to this fractional ideal, since $p^m\omega_1, \ldots, p^m\omega_s$ form a $\mathbb{Z}$-basis for $p^m\mathcal{O}_F$. □

Lemma 2.6. *For any rational primes p and q, there exists a degree-p cyclic extension $E/\mathbb{Q}$ in which q splits completely. If moreover p is odd, then any such E is totally real.*

Proof. Choose a rational prime ℓ splitting completely in $\mathbb{Q}(e^{2\pi i/p}, q^{1/p})$. Then $\ell \equiv 1 \pmod{p}$ and the image of q in $(\mathbb{Z}/\ell\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/\ell})/\mathbb{Q})$ is a p-th power. Equivalently, the Frobenius automorphism $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/\ell})/\mathbb{Q})$ belongs to the index-p subgroup H of the cyclic group $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/\ell})/\mathbb{Q})$. Let E be the subfield of $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/\ell})/\mathbb{Q})$ fixed by H. Then the image of Frob_q in $\mathrm{Gal}(E/\mathbb{Q})$ is trivial, so q splits completely in E. Odd-degree Galois extensions of $\mathbb{Q}$ are totally real. □

2.2. **Notation and Assumptions.** We view all number fields as being subfields of a fixed algebraic closure $\overline{\mathbb{Q}}$, so that compositums are well-defined.

- Let K be the number field given in Theorem 1.8. Thus K is totally real, or K is a totally complex degree-2 extension of a totally real field.
- Let $n = [K : \mathbb{Q}]$.
- Let $\mathfrak{p}$ be the prime of K in Theorem 1.8.
- Let $p_{\mathbb{Q}}$ be the prime of $\mathbb{Q}$ below $\mathfrak{p}$.
- Let $p = p_0 < p_1 < \cdots < p_n$ be a sequence of odd primes such that $p_i > n$ and $1/p_i < \varepsilon/(n+1)$ for all i.
- Let $E = E_0, E_1, \ldots, E_n$ be a sequence of totally real cyclic extensions of $\mathbb{Q}$ such that $[E_i : \mathbb{Q}] = p_i$ and $p_{\mathbb{Q}}$ splits completely in E. (These exist by Lemma 2.6.)
- Let L be an imaginary degree-2 extension of $\mathbb{Q}$ in which $p_{\mathbb{Q}}$ splits completely. (For instance, let $b < 0$ be an integer that is a nonzero square mod $p_{\mathbb{Q}}$ and let $L = \mathbb{Q}(\sqrt{b})$.)
- Let $\mathcal{V}_{\mathbb{Q}}$ be the set of rational primes that are inert in all of the extensions $E_i/\mathbb{Q}$ for $0 \le i \le n$. Let $\mathcal{W}_{\mathbb{Q}} = \mathcal{V}_{\mathbb{Q}} \cup \{p_{\mathbb{Q}}\}$.
- Let $\mathcal{W}_{EL}$ be the set of EL-primes above $\mathcal{W}_{\mathbb{Q}}$.
- Let $\mathcal{W}_K$ be the set of K-primes above $\mathcal{W}_{\mathbb{Q}}$.
- Let σ_L, σ_E be generators of $\mathrm{Gal}(L/\mathbb{Q})$, $\mathrm{Gal}(E/\mathbb{Q})$ respectively.
- Let $\mathfrak{p}_{EL}$ be a prime above $p_{\mathbb{Q}}$ in EL.
- Let $\Omega = \{\omega_1, \ldots, \omega_{2p}\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_{EL}$. Then Ω is also an $\mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$-basis for $\mathcal{O}_{EL,\mathcal{W}_{EL}}$.

2.3. **Discrete Diophantine subsets of large subrings of $\mathbb{Q}$.** The following proposition provides the foundation for our construction.

Proposition 2.7. *Let $x \in \mathcal{O}_{EL,\mathcal{W}_{EL}}$ be a solution to the system*

$$\begin{cases} N_{EL/L}(x) = 1, \\ N_{EL/E}(x) = 1. \end{cases} \tag{1}$$

such that

$$x \text{ is a unit at all primes of } EL \text{ above } p_{\mathbb{Q}} \text{ except possibly for } \mathfrak{p}_{EL},\ \sigma_E(\mathfrak{p}_{EL}),\ \sigma_L(\mathfrak{p}_{EL}), \text{ and } \sigma_E\sigma_L(\mathfrak{p}_{EL}) = \sigma_L\sigma_E(\mathfrak{p}_{EL}); \text{ and} \tag{2}$$

$$\mathrm{ord}_{\mathfrak{p}_{EL}} x > 0 \text{ and } \mathrm{ord}_{\sigma_E\sigma_L(\mathfrak{p}_{EL})} x > 0. \tag{3}$$

Then the divisor of x equals

$$\left(\frac{\mathfrak{p}_{EL}\,\sigma_E\sigma_L(\mathfrak{p}_{EL})}{\sigma_E(\mathfrak{p}_{EL})\,\sigma_L(\mathfrak{p}_{EL})}\right)^k \tag{4}$$

for some $k \in \mathbb{Z}_{>0}$. Furthermore, the set of solutions to (1) *satisfying* (2) *and* (3) *is nonempty and closed under multiplication. If x_1 and x_2 are solutions to* (1)*, then x_1/x_2 is again a solution to* (1)*, but x_1/x_2 will not necessarily satisfy* (2) *and* (3) *even if x_1 and x_2 do.*

Proof. Since $p_{\mathbb{Q}}$ splits completely in E and in L, it splits completely in EL. Now apply Section 3.3.2 on page 131 of [Shl00b]. □

Corollary 2.8. *Let A be the set of $(a_1, \dots, a_{2p})$ in $\left(\mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}\right)^{2p}$ such that the element $x = \sum_{i=1}^{2p} a_i\omega_i$ of $\mathcal{O}_{EL,\mathcal{W}_{EL}}$ satisfies* (1), (2), *and* (3). *Let B be the set of $b \in \mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$ such that for some $(a_1, \dots, a_{2p}) \in A$,*

(i) *The element b equals one of the a_i, and*
(ii) $\operatorname{ord}_{p_{\mathbb{Q}}} b = \min\{\operatorname{ord}_{p_{\mathbb{Q}}} a_1, \dots, \operatorname{ord}_{p_{\mathbb{Q}}} a_{2p}\}$.

(Thus B is the set of "$p_{\mathbb{Q}}$-adically largest coordinates" of elements of A.) For $r \in \mathbb{Z}$, let $B_r = \{\, b \in B : \operatorname{ord}_{p_{\mathbb{Q}}} b = r \,\}$. Then

(1) *A and B are Diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$.*
(2) *There exists $M \in \mathbb{Z}_{>0}$ such that $B = \bigcup_{m=1}^{\infty} B_{-Mm}$ and each B_{-Mm} in the union is a nonempty finite set.*

Proof.

(1) By writing each norm in (1) as a product of conjugates, we find that the equations (1) are equivalent to polynomial equations in the a_i. By Corollary 2.3 together with the "Going up and then down" method (see Section 2.2 of [Shl00b]), conditions (2) and (3) are Diophantine. Thus A is Diophantine.

Condition (i) is $\prod_{i=1}^{2p}(b-a_i) = 0$, and condition (ii) is Diophantine by Corollary 2.3, so B is Diophantine too.

(2) If $b \in B$ is associated to $(a_1, \dots, a_{2p}) \in A$ and k is the positive integer in (4) for the element $x = \sum_{i=1}^{2p} a_i\omega_i$, then $\operatorname{ord}_{p_{\mathbb{Q}}} b = -k$ by Lemma 2.5. Thus the set of r for which $B_r \neq \emptyset$ equals the set of possibilities for $-k$ in (4) as x varies over all solutions to (1) satisfying (2) and (3). Let M be the smallest positive integer such that $-M$ is a possible value of $-k$. Proposition 2.7 implies that the set of possibilities for $-k$ is then $\{-M, -2M, \dots\}$. Thus $B_r \neq \emptyset$ if and only if $r \in \{-M, -2M, \dots\}$.

It remains to prove that each B_r is finite. Fix $r \in \mathbb{Z}$. The finiteness of B_r follows once we show that the set of x satisfying (1), (2), and (3) and having $k = -r$ in (4) is finite. Suppose x_1 and x_2 are two such values of x, so by (4) the divisor of x_1/x_2 is trivial. Then $x_1/x_2 \in \mathcal{O}_{EL}^*$ and $N_{EL/E}(x_1/x_2) = 1$. But EL/E is a totally complex degree-2 extension of a totally real field, so these conditions imply that x_1/x_2 is a root of unity. Finally, there are only finitely many roots of unity in EL.

□

Corollary 2.9. *There exists an infinite Diophantine subset B of $\mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$ that is $p_{\mathbb{Q}}$-adically discrete and closed.*

Proof. The Diophantine set B of Corollary 2.8 is infinite, because it is an infinite disjoint union of nonempty sets. It is $p_{\mathbb{Q}}$-adically discrete and closed, because for each $r < 0$, the set of $b \in B$ with $\operatorname{ord}_{p_{\mathbb{Q}}} b \geq r$ is finite. □

2.4. **Discrete Diophantine subsets of large subrings of K.**

Proposition 2.10. *Let $\mathcal{U}$ be a set of K-primes remaining prime in E_iK/K for $i = 0, \ldots, n$. Then there exists a set of K-primes $\bar{\mathcal{U}}$ such that the set difference $(\mathcal{U} - \bar{\mathcal{U}}) \cup (\bar{\mathcal{U}} - \mathcal{U})$ is finite and $\mathcal{O}_{K,\bar{\mathcal{U}}} \cap \mathbb{Q}$ has a Diophantine definition over $\mathcal{O}_{K,\bar{\mathcal{U}}}$.*

Proof. See Corollary 2.3 and Theorem 3.8 of [Shl02]. (The application of Corollary 2.3 requires that p_i does not divide the absolute degree of the Galois closure of $K/\mathbb{Q}$; this holds since $p_i > n$.) □

Clearly Proposition 2.10 implies the slightly stronger version in which the hypothesis on $\mathcal{U}$ is weakened to the hypothesis that *all but finitely many* primes of $\mathcal{U}$ are inert in all the E_iK/K. We now show that we can also insist that the new set of primes contains the original set:

Proposition 2.11. *Let $\mathcal{U}$ be a set of K-primes such that all but finitely many of them are inert in E_iK/K for $i = 0, \ldots, n$. Then there exists a set of K-primes $\mathcal{U}'$* containing $\mathcal{U}$ *such that $\mathcal{U}' - \mathcal{U}$ is finite and $\mathcal{O}_{K,\mathcal{U}'} \cap \mathbb{Q}$ is Diophantine over $\mathcal{O}_{K,\mathcal{U}'}$.*

Proof. Let $\bar{\mathcal{U}}$ be the set given by (the slightly stronger version of) Proposition 2.10, and let $\mathcal{U}' = \mathcal{U} \cup \bar{\mathcal{U}}$. Thus $\mathcal{U}' - \mathcal{U}$ is finite.

By choice of $\bar{\mathcal{U}}$, the set $R := \mathcal{O}_{K,\bar{\mathcal{U}}} \cap \mathbb{Q}$ is Diophantine over $\mathcal{O}_{K,\bar{\mathcal{U}}}$, which is Diophantine over $\mathcal{O}_{K,\mathcal{U}'}$ by Proposition 2.4. Thus R is a Diophantine subset of $\mathcal{O}_{K,\mathcal{U}'}$. The desired subset $\mathcal{O}_{K,\mathcal{U}'} \cap \mathbb{Q}$ can now be defined as the set of elements of $\mathcal{O}_{K,\mathcal{U}'}$ equal to a ratio of elements of R with nonzero denominator (here we use Proposition 2.1 for R). □

Proof of Theorem 1.8. We will apply Proposition 2.11 to the set $\mathcal{W}_K$ defined in Section 2.2. By assumption, the cyclic extension $E_i/\mathbb{Q}$ has prime degree $p_i > n$. Thus $[E_iK : K] = p_i$, and moreover, a K-prime is inert in E_iK/K if and only if the $\mathbb{Q}$-prime below it is inert in $E_i/\mathbb{Q}$. All primes of $\mathcal{W}_{\mathbb{Q}}$ but $p_{\mathbb{Q}}$ are inert in all the $E_i/\mathbb{Q}$, so all primes of $\mathcal{W}_K$ but finitely many are inert in all the E_iK/K. Thus we may apply Proposition 2.11 to find a set of K-primes $\mathcal{W}'_K$ such that $\mathcal{W}'_K - \mathcal{W}_K$ is finite and such that the set $\mathcal{O}_{\mathbb{Q},\mathcal{W}'_{\mathbb{Q}}}$ is Diophantine over $\mathcal{O}_{K,\mathcal{W}'_K}$, where $\mathcal{W}'_{\mathbb{Q}}$ is the set of $\mathbb{Q}$-primes q such that all K-primes above q lie in $\mathcal{W}'_K$.

Since $\mathcal{W}'_K - \mathcal{W}_K$ is finite, $\mathcal{W}'_{\mathbb{Q}} - \mathcal{W}_{\mathbb{Q}}$ is finite.

Now the infinite set B of Corollary 2.9 is Diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$, which by Proposition 2.4 is Diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}'_{\mathbb{Q}}}$, which is Diophantine over $\mathcal{O}_{K,\mathcal{W}'_K}$. Thus B is Diophantine over $\mathcal{O}_{K,\mathcal{W}'_K}$. Since $\mathfrak{p}$ lies above $p_{\mathbb{Q}}$, the set B is $\mathfrak{p}$-adically discrete and closed. To fulfill the requirements of Theorem 1.8, we take $\mathcal{S} = \mathcal{W}'_K$. This is recursive, since up to a finite set, its primes are characterized by splitting behavior in a finite list of extension fields.

It remains to show that $\mathcal{W}'_K$ has density greater than $1-\varepsilon$. Up to finitely many primes, $\mathcal{W}'_K$ is defined by the splitting behavior in finitely many extensions of K (namely, the E_iK/K). Thus, by the Chebotarev Density Theorem (see Théorème 1 of [Ser81] for a version using natural density), $\mathcal{W}'_K$ has a density. The density of the set of K-primes that *fail* to be inert in E_iK/K is $1/p_i$, so the density of $\mathcal{W}'_K$ is at least

$$1 - \sum_{i=0}^{n} \frac{1}{p_i} \; > \; 1 - \sum_{i=0}^{n} \frac{\varepsilon}{n+1} \; = \; 1 - \varepsilon.$$

□

3. Using Elliptic Curves

3.1. **Notation.**

- Whenever k is a perfect field, let $\overline{k}$ be an algebraic closure, and let $G_k = \operatorname{Gal}(\overline{k}/k)$.
- K is a number field.
- E is an elliptic curve of rank 1 over K. (In particular, we assume that K is such that such an E exists).
- We fix a Weierstrass equation $y^2 = x^3 + ax + b$ for E with coefficients in the ring of integers of K.
- $E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$.
- r is an even multiple of $\#E(K)_{\text{tors}}$.
- $Q \in E(K)$ is such that Q generates $E(K)/E(K)_{\text{tors}}$.
- $P := rQ$.
- $\mathcal{P}_{\mathbb{Q}} = \{2, 3, 5, \dots\}$ is the set of rational primes.
- $\mathcal{P}_K$ is the set of all finite primes of K.
- Let $\mathcal{S}_{\text{bad}} \subseteq \mathcal{P}_K$ consist of the primes that ramify in $K/\mathbb{Q}$, the primes for which the reduction of the chosen Weierstrass model is singular (this includes all primes above 2), and the primes at which the coordinates of P are not integral. We occasionally view E as the scheme over $\mathcal{O}_{K,\mathcal{S}_{\text{bad}}}$ defined by the homogenization of the Weierstrass equation.
- E' is the smooth affine curve $y^2 = x^3 + ax + b$ over $\mathcal{O}_{K,\mathcal{S}_{\text{bad}}}$. Thus E' is E with the zero section removed.
- $\mathcal{M}_K$ is the set of all normalized absolute values of K.
- $\mathcal{M}_{K,\infty} \subset \mathcal{M}_K$ is the set of all archimedean absolute values of K.
- For $\mathfrak{p} \in \mathcal{P}_K$, let
  1. $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$.
  2. $R_{\mathfrak{p}}$ be the valuation ring of $K_{\mathfrak{p}}$
  3. $\mathbb{F}_{\mathfrak{p}}$ be the residue field of $R_{\mathfrak{p}}$,
  4. $\mathbf{N}\mathfrak{p} = \#\mathbb{F}_{\mathfrak{p}}$ be the absolute norm of $\mathfrak{p}$
- Write $nP = (x_n, y_n)$ where $x_n, y_n \in K$.
- Let the divisor of x_n be of the form

  $$\frac{\mathfrak{a}_n}{\mathfrak{d}_n}\mathfrak{b}_n,$$

  where
  - $\mathfrak{d}_n = \prod_{\mathfrak{q}} \mathfrak{q}^{-a_{\mathfrak{q}}}$, where the product is taken over all primes $\mathfrak{q}$ of K not in $\mathcal{S}_{\text{bad}}$ such that $a_{\mathfrak{q}} = \operatorname{ord}_{\mathfrak{q}} x_n < 0$,
  - $\mathfrak{a}_n = \prod_{\mathfrak{q}} \mathfrak{q}^{a_{\mathfrak{q}}}$, where the product is taken over all primes $\mathfrak{q}$ of K not in $\mathcal{S}_{\text{bad}}$ such that $a_{\mathfrak{q}} = \operatorname{ord}_{\mathfrak{q}} x_n > 0$.
  - $\mathfrak{b}_n = \prod_{\mathfrak{q}} \mathfrak{q}^{a_{\mathfrak{q}}}$, where the product is taken over all primes $\mathfrak{q} \in \mathcal{S}_{\text{bad}}$ and $a_{\mathfrak{q}} = \operatorname{ord}_{\mathfrak{q}} x_n$.

- For n as above, let $\mathcal{S}_n = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} | \mathfrak{d}_n\}$. By definition of $\mathcal{S}_{\text{bad}}$, we have $\mathcal{S}_1 = \emptyset$.
- For n as above, let $d_n = \mathbf{N}\mathfrak{d}_n \in \mathbb{Z}_{\geq 1}$.
- For $u \in K^*$ and v a place of K lying above the place p of $\mathbb{Q}$ (possibly $p = \infty$), define the (unnormalized) local height $h_v(u) = \log \max\{\|u\|_v, 1\}$ where $\|u\|_v = |\mathbf{N}_{K_v/\mathbb{Q}_p}(u)|_p$ and K_v and $\mathbb{Q}_p$ denote completions.
- For $u \in K^*$, define the global height $h(u) = \sum_{v \in \mathcal{M}_K} h_v(u)$.
- For $\ell \in \mathcal{P}_{\mathbb{Q}}$, define a_ℓ to be the smallest positive number such that $\mathcal{S}_{\ell^{a_\ell}} \neq \emptyset$. (By Siegel's Theorem, $a_\ell = 1$ for all but finitely many ℓ.)
- Let $\mathcal{L} = \{\ell \in \mathcal{P}_{\mathbb{Q}} : a_\ell > 1\}$ and $L = \prod_{\ell \in \mathcal{L}} \ell^{a_\ell - 1}$.
- Let $\mathfrak{p}_\ell$ be a prime of largest norm in $\mathcal{S}_{\ell^{a_\ell}}$.
- For $\ell, m \in \mathcal{P}_{\mathbb{Q}}$, let $\mathfrak{p}_{\ell m}$ be a prime of largest norm in $\mathcal{S}_{\ell m} - (\mathcal{S}_\ell \cup \mathcal{S}_m)$, if this set is nonempty (see Proposition 3.5).
- $E[m]$ denotes $\{\, T \in E(\overline{K}) : mT = 0 \,\}$.
- If λ is an ideal in the endomorphism ring of E, then
$$E[\lambda] := \{\, T \in E(\overline{K}) : aQ = 0 \text{ for some } a \in \lambda \,\}.$$

3.2. **Divisibility of denominators of x-coordinates.** The next lemma is the number field analogue to Lemma 3.1(a) of [Poo03], where it was proved for $\mathbb{Q}$.

Lemma 3.1. *Let $P \in E(K) - \{0\}$ be of infinite order and let $n \in \mathbb{Z} - \{0\}$. Let $\mathfrak{r}$ be an integral divisor of K. Then $\{n \in \mathbb{Z} : \mathfrak{r} \mid \mathfrak{d}_n(P)\}$ is a subgroup of $\mathbb{Z}$.*

Proof. It is enough to prove the lemma when $\mathfrak{r}$ is a prime power $\mathfrak{p}^m$. Let $\hat{E}$ be the formal group over $R_\mathfrak{p}$ defined by the chosen Weierstrass model of E. Let $\hat{E}(\mathfrak{p}R_\mathfrak{p})$ be the group of points associated to $\hat{E}$. There exist Laurent series $x(z) = z^{-2} + \cdots$ and $y(z) = z^{-3} + \cdots$ with coefficients in $R_\mathfrak{p}$ giving an injective homomorphism $\hat{E}(\mathfrak{p}R_\mathfrak{p}) \to E(K_\mathfrak{p})$ whose image is the set $E_1(K_\mathfrak{p})$ of $(x, y) \in E(K_\mathfrak{p})$ with $\operatorname{ord}_\mathfrak{p}(x) < 0$ (together with O): this follows from Proposition VII.2.2 of [Sil92] when the Weierstrass equation is minimal, but the proof there does not use the minimality. Since $\operatorname{ord}_\mathfrak{p} x(z) = -2 \operatorname{ord}_\mathfrak{p} z$ whenever $z \in \mathfrak{p}R_\mathfrak{p}$, the set of $(x, y) \in E(K_\mathfrak{p})$ with $\operatorname{ord}_\mathfrak{p}(x) \leq -m$ (together with O) corresponds under this homomorphism to a subgroup $\mathfrak{p}^{\lceil m/2 \rceil} R_\mathfrak{p}$ of $\mathfrak{p}R_\mathfrak{p}$, and hence is a subgroup of $E(K_\mathfrak{p})$. □

Corollary 3.2. *Let $m, n \in \mathbb{Z} - \{0\}$, and let (m, n) be their gcd. Then $\mathcal{S}_m \cap \mathcal{S}_n = \mathcal{S}_{(m,n)}$. In particular, if $(m, n) = 1$ then $\mathcal{S}_m \cap \mathcal{S}_n = \emptyset$.*

3.3. **New primes in denominators of x-coordinates.**

Lemma 3.3. *Let $n \in \mathbb{Z}_{\geq 1}$. Suppose that $\mathfrak{t} \in \mathcal{P}_K$ divides $\mathfrak{d}_n$, and $p \geq 3$ is a rational prime.*

1. *If $\mathfrak{t} \mid p$, then* $\operatorname{ord}_\mathfrak{t} \mathfrak{d}_{pn} = \operatorname{ord}_\mathfrak{t} \mathfrak{d}_n + 2$.
2. *If $\mathfrak{t} \nmid p$, then* $\operatorname{ord}_\mathfrak{t} \mathfrak{d}_{pn} = \operatorname{ord}_\mathfrak{t} \mathfrak{d}_n$.

Proof. We will use the notation of Lemma 3.1. Since $\mathfrak{t} \mid \mathfrak{d}_n$, by assumption $\mathfrak{t} \notin \mathcal{S}_{\text{bad}}$. In particular $\mathfrak{t}$ is not ramified over $\mathbb{Q}$. Furthermore, $\operatorname{ord}_\mathfrak{t} x_n < 0$, so $nP \in E_1(K_\mathfrak{t})$. Let z be the corresponding element in the group of points $\hat{E}(\mathfrak{t}R_\mathfrak{t})$ of the formal group. We have $[p]z = pf(z) + g(z^p)$, by Proposition 2.3, page 116 and Corollary 4.4, page 120 of [Sil92], where $[p]$ is the multiplication-by-p in the formal group and $f(T), g(T) \in R_\mathfrak{t}[[T]]$ satisfy $g(0) = 0$ and $f(T) = T +$ higher order terms. Thus $\operatorname{ord}_\mathfrak{t}([p]z)$ equals $(\operatorname{ord}_\mathfrak{t} z) + 1$ or $\operatorname{ord}_\mathfrak{t} z$, depending on whether $\mathfrak{t} \mid p$. Since $x = z^{-2} + \cdots$, we find that $\operatorname{ord}_\mathfrak{t} x_{pn}$ equals $(\operatorname{ord}_\mathfrak{t} x_n) - 2$ or $\operatorname{ord}_\mathfrak{t} x_n$, depending on whether $\mathfrak{t} \mid p$. □

Lemma 3.4. *There exists $c \in \mathbb{R}_{>0}$ such that $\log d_n = (c - o(1))n^2$ as $n \longrightarrow \infty$.*

Proof. Let $\hat{h}$ be the canonical height on $E(K)$. Then $\hat{h}(nP)/n^2$ is a positive constant independent of n. The Weil height differs from $\hat{h}$ by $O(1)$, so $h(x_n)/n^2$ tends to a positive limit as $n \to \infty$. By definition, $h(x_n)$ differs from $\log d_n$ by the sum of $h_v(x_n)$ over archimedean v and $v \in \mathcal{S}_{\text{bad}}$. By the theorem on page 101 of [Ser97], $h_v(x_n)/h(x_n) \to 0$ as $n \to \infty$ for each v, so $(\log d_n)/h(x_n)$ tends to 1 as $n \to \infty$. Thus $(\log d_n)/n^2$ tends to a positive limit as $n \to \infty$. □

The next proposition is a number field version of Lemma 3.4 of [Poo03].

Proposition 3.5. *If $\ell, m \in \mathcal{P}_{\mathbb{Q}}$ and $\max(\ell, m)$ is sufficiently large, then $\mathcal{S}_{\ell m} - (\mathcal{S}_\ell \cup \mathcal{S}_m) \neq \emptyset$.*

Proof. Suppose $\mathcal{S}_{\ell m} - (\mathcal{S}_\ell \cup \mathcal{S}_m) = \emptyset$. We claim that $\mathfrak{d}_{\ell m} \mid \ell^2 m^2 \mathfrak{d}_\ell \mathfrak{d}_m$. To check this, we compare orders of both sides at a prime $\mathfrak{t}$ dividing $\mathfrak{d}_{\ell m}$. By assumption, $\mathfrak{t}$ divides either $\mathfrak{d}_\ell$ or $\mathfrak{d}_m$. Without loss of generality, assume $\mathfrak{t} \mid \mathfrak{d}_\ell$. Then Lemma 3.3 implies $\operatorname{ord}_{\mathfrak{t}} \mathfrak{d}_{\ell m} \leq \operatorname{ord}_{\mathfrak{t}}(m^2 \mathfrak{d}_\ell)$, which proves the claim.

Taking norms, we obtain $d_{\ell m} \mid (\ell m)^{2[K:\mathbb{Q}]} d_\ell d_m$. Taking logs and applying Lemma 3.4, we deduce

$$\begin{aligned}(c - o(1))\ell^2 m^2 &\leq 2[K : \mathbb{Q}](\log \ell + \log m) + (c - o(1))\ell^2 + (c - o(1))m^2 \\ &\leq (c + o(1))(\ell^2 + m^2),\end{aligned}$$

which is a contradiction once ℓ and m are both sufficiently large. □

3.4. **Density of prime multiples.**

Lemma 3.6. *Let $\vec{\alpha} \in \mathbb{R}^n$, let I be an open neighborhood of 0 in $\mathbb{R}^n/\mathbb{Z}^n$, and let $d \in \mathbb{Z}_{\geq 1}$. Then the set of primes $\ell \equiv 1 \pmod{d}$ such that $(\ell - 1)\vec{\alpha} \bmod 1$ is in I has positive upper density.*

Proof. Let $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$. We first reduce to the case that $1, \alpha_1, \ldots, \alpha_n$ are $\mathbb{Z}$-independent. Choose $m \in \mathbb{Z}_{\geq 1}$ and $\beta_1, \ldots, \beta_r$ such that $1/m, \beta_1, \ldots, \beta_r$ form a $\mathbb{Z}$-basis for the subgroup of $\mathbb{R}$ generated by $1, \alpha_1, \ldots, \alpha_n$. Replacing d by a positive integer multiple only reduces the density, so we may assume $m \mid d$. For fixed i, if $\alpha_i = \frac{c_0}{m} + \sum_{j=1}^r c_j \beta_j$, then for $\ell \equiv 1 \pmod{d}$ we have

$$(\ell - 1)\alpha_i \equiv \sum_{j=1}^r c_j (\ell - 1)\beta_j \pmod{1},$$

so it suffices to prove positivity of the upper density of $\ell \equiv 1 \pmod{d}$ for which $(\ell - 1)\beta_j$ is sufficiently close mod 1 to 0 for all j.

In fact, we will prove the stronger result that the points $(\ell - 1)\vec{\beta} \in (\mathbb{R}/\mathbb{Z})^r$ for prime $\ell \equiv 1 \pmod{d}$ are equidistributed. By Weyl's equidistribution criterion [Wey16, Satz 3], we reduce to proving that for any $\alpha \in \mathbb{R} - \mathbb{Q}$,

$$\sum_{\substack{\ell \leq x \\ \ell \equiv 1 \pmod{d}}} e^{2\pi i \ell \alpha} = o(\pi(x))$$

as $x \to \infty$. This is a consequence of Vinogradov's work on exponential sums over primes: see [Mon94, p. 34], for instance. □

3.5. **Denominators of x-coordinates having many small prime factors.** We next prove an analogue of Lemma 7.1 of [Poo03] showing that it is rare that $\mathcal{S}_\ell$ has a large fraction of the small primes. For prime ℓ, define

$$\mu_\ell = \sup_{X \in \mathbb{Z}_{\geq 2}} \frac{\#\{\mathfrak{p} \in \mathcal{S}_\ell : \mathbf{N}\mathfrak{p} \leq X\}}{\#\{\mathfrak{p} \in \mathcal{P}_K : \mathbf{N}\mathfrak{p} \leq X\}}.$$

Lemma 3.7. *For any $\varepsilon > 0$, the density of $\{\, \ell : \mu_\ell > \varepsilon \,\}$ is* 0.

Proof. The proof can be copied from that of Lemma 7.1 of [Poo03], using "the primes $\mathfrak{p} \in \mathcal{P}_K$ with $\mathbf{N}\mathfrak{p} \leq X$" everywhere in place of the "the primes p up to X": it requires only the facts

(1) The function $\pi_K(X) := \#\{\mathfrak{p} \in \mathcal{P}_K : \mathbf{N}\mathfrak{p} \leq X\}$ is $(1 + o(1))X/\log X$ as $X \to \infty$ (Theorem 3 on page 213 of [CF86]).
(2) $\#\mathcal{S}_\ell \leq \log_2 d_\ell$ (clear, since each prime has norm at least 2)
(3) $\log_2 d_\ell = O(\ell^2)$ as $\ell \to \infty$ (follows from Lemma 3.4).

□

3.6. **Construction of the ℓ_i.** By [Sil92, Corollary VI.5.1.1] and [Sil94, Corollary V.2.3.1], there is an isomorphism of real Lie groups $\prod_{v \in \mathcal{M}_{K,\infty}} E(K_v) \simeq (\mathbb{R}/\mathbb{Z})^N \times (\mathbb{Z}/2\mathbb{Z})^{N'}$ for some $N \geq 1$ and $N' \geq 0$. Fix such an isomorphism, and embed $E(K)$ diagonally in $\prod_{v \in \mathcal{M}_{K,\infty}} E(K_v)$. Since $P = rQ$ with r even, the point P maps to an element $\vec{\alpha} \in (\mathbb{R}/\mathbb{Z})^N$.

Define a sequence of primes ℓ_i inductively as follows. Given $\ell_1, \ldots, \ell_{i-1}$, let ℓ_i be the smallest prime outside $\mathcal{L}$ and exceeding the bound implicit in Proposition 3.5 such that all of the following hold:

(1) $\ell_i > \ell_j$ for all $j < i$,
(2) $\mu_{\ell_i} \leq 2^{-i}$,
(3) $\mathbf{N}\mathfrak{p}_{\ell_i \ell_j} > 2^i$ for all $j < i$,
(4) $\mathbf{N}\mathfrak{p}_{\ell \ell_i} > 2^i$ for all $\ell \in \mathcal{L}$,
(5) $\ell_i \equiv 1 \pmod{i!}$, and
(6) $|x_{\ell_i - 1}|_v > i$ for all $v \in \mathcal{M}_{K,\infty}$.

Proposition 3.8. *The sequence $\ell_1, \ell_2, \ldots$ is well-defined and computable.*

Proof. Condition (6) is equivalent to the requirement that $(\ell - 1)\vec{\alpha}$ lie in a certain open neighborhood of 0 in $(\mathbb{R}/\mathbb{Z})^N$, since the Lie group isomorphism maps neighborhoods of O to neighborhoods of 0. Thus by Lemma 3.6, the set of primes satisfying (5) and (6) has positive upper density. By Lemma 3.7, (2) fails for a set of density 0. Therefore it will suffice to show that (1), (3), and (4) are satisfied by all sufficiently large ℓ_i.

For fixed $j \leq i$, the primes $\mathfrak{p}_{\ell_i \ell_j}$ for varying values of ℓ_i are distinct by Corollary 3.2, so eventually their norms are greater than 2^i. The same holds for $\mathfrak{p}_{\ell \ell_i}$ for fixed $\ell \in \mathcal{L}$. Thus by taking ℓ_i sufficiently large, we can make all the $\mathfrak{p}_{\ell_i \ell_j}$ and $\mathfrak{p}_{\ell \ell_i}$ have norm greater than 2^i. Thus the sequence is well-defined.

Each ℓ_i can be computed by searching primes in increasing order until one is found satisfying the conditions: condition (6) can be tested effectively, since $|x_{\ell_i - 1}|_v$ is an algebraic real number. □

As in Section 4 of [Poo03], we define the following subsets of $\mathcal{P}_K$:

- $\mathcal{T}_1 = \mathcal{S}_{\text{bad}} \cup \bigcup_{i \geq 1} \mathcal{S}_{\ell_i}$,

- $\mathcal{T}_2^a$ is the set of $\mathfrak{p}_\ell$ for $\ell \notin \{\ell_1, \ell_2, \dots\}$,
- $\mathcal{T}_2^b = \{\, \mathfrak{p}_{\ell_i \ell_j} : 1 \le j \le i \,\}$,
- $\mathcal{T}_2^c = \{\, \mathfrak{p}_{\ell \ell_i} : \ell \in \mathcal{L}, i \ge 1 \,\}$, and
- $\mathcal{T}_2 = \mathcal{T}_2^a \cup \mathcal{T}_2^b \cup \mathcal{T}_2^c$.

As in Section 5 of [Poo03], we prove that

Lemma 3.9. *The sets $\mathcal{T}_1$ and $\mathcal{T}_2$ are disjoint. If the subset $\mathcal{S} \subset \mathcal{P}_K$ contains $\mathcal{T}_1$ and is disjoint from $\mathcal{T}_2$, then $\mathcal{E} := E'(\mathcal{O}_{K,\mathcal{S}}) \cap rE(K)$ is the union of $\{\, \pm \ell_i P : i \ge 1 \,\}$ and some subset of the finite set $\{\, sP : s \mid \prod_{\ell \in \mathcal{L}} \ell^{a_\ell - 1} \,\}$.*

Proof. Once we note that $rE(K) = \mathbb{Z}P$, the proofs proceed as in Section 5 of [Poo03]. □

The recursiveness of $\mathcal{T}_1$ and $\mathcal{T}_2$ follows as in Section 8 of [Poo03], using the following:

Lemma 3.10. *If ℓ is prime, then $\ell \mid \#E(\mathbb{F}_{\mathfrak{p}_\ell})$.*

Proof. For $\mathfrak{p} \notin \mathcal{S}_{\text{bad}}$, a multiple nP reduces to 0 in $E(\mathbb{F}_\mathfrak{p})$ if and only if $\mathfrak{p}$ divides $\mathfrak{d}_n$. Hence, by definition of $\mathfrak{p}_\ell$, the point $\ell^{a_\ell} P$ reduces to 0 in $E(\mathbb{F}_{\mathfrak{p}_\ell})$ but $\ell^{a_\ell - 1} P$ does not. □

3.7. **Density of $\mathcal{T}_1$ and $\mathcal{T}_2$.** The proofs that $\mathcal{T}_1$, $\mathcal{T}_2^b$, and $\mathcal{T}_2^c$ have density 0 are identical to the proofs in Section 9 of [Poo03]. The remainder of this section is devoted to proving that $\mathcal{T}_2^a$ has density 0. Again, we follow [Poo03], but more work is necessary because we no longer assume that E has no CM.

For $n \in \mathbb{Z}_{>0}$, let $\omega(n)$ be the number of distinct prime factors of n.

Lemma 3.11. *For any $t \ge 1$, the density of $\{\, \mathfrak{p} : \omega(\#E(\mathbb{F}_\mathfrak{p})) < t \,\}$ is 0.*

Proof. If E does not have CM (i.e., $\operatorname{End} E_{\overline{K}} = \mathbb{Z}$), then the proof given for $K = \mathbb{Q}$ in Lemma 9.3 of [Poo03] generalizes easily to arbitrary K. The first step in this proof, which we will also use for the CM case, is to relate divisibility to Galois representations: namely, for a prime $\mathfrak{p}$ of good reduction not above ℓ, the condition $\ell \mid \#E(\mathbb{F}_\mathfrak{p})$ is equivalent to the existence of an ℓ-torsion point in $E(\overline{\mathbb{F}}_\mathfrak{p})$ fixed by the Frobenius element of $\operatorname{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$, which in turn is equivalent to the condition that the the image of a Frobenius element at $\mathfrak{p}$ under $G_K \to \operatorname{Aut} E[\ell] = \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has a nontrivial fixed vector in $(\mathbb{Z}/\ell\mathbb{Z})^2$.

We assume from now on that E has CM, say by an order $\mathcal{O}$ in a quadratic imaginary field F. Using the action of $\mathcal{O}$ on $\operatorname{Lie} E$ (the tangent space of E at O), we may view $\mathcal{O}$ (and hence also F) as a subring of $\overline{K}$.

All the endomorphisms are defined over the compositum KF [Sil94, II.2.2(b)].

Let Λ be the set of primes ℓ of $\mathbb{Z}$ such that $\ell \nmid \operatorname{disc}(\mathcal{O})$ and (ℓ) factors into distinct prime ideals λ and $\bar{\lambda}$ of $\mathcal{O}$. (Later we will delete finitely many primes from Λ.)

For $\ell \in \Lambda$,

$$E[\ell] = E[\lambda] \oplus E[\bar{\lambda}].$$

The summands on the right are free modules over $\mathcal{O}/\lambda$ and $\mathcal{O}/\bar{\lambda}$, respectively, and we choose generators for each in order to obtain identifications

$$E[\ell] \simeq \mathcal{O}/\lambda \oplus \mathcal{O}/\bar{\lambda} \simeq (\mathbb{Z}/\ell\mathbb{Z})^2,$$

and hence $\operatorname{Aut} E[\ell] \simeq \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The action of G_{KF} commutes with the $\mathcal{O}$-action, so the image of G_{KF} in $\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ lies in the subgroup $\begin{pmatrix} * & \\ & * \end{pmatrix}$ of diagonal matrices. On the other hand, if $\tau \in G_K - G_{KF}$, then τ interchanges λ and $\bar{\lambda}$, and its image in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ lies in the coset $\begin{pmatrix} & * \\ * & \end{pmatrix}$.

Define subgroups

$$D = \begin{pmatrix} * & \\ & * \end{pmatrix}$$

$$H = \begin{pmatrix} * & \\ & * \end{pmatrix} \cup \begin{pmatrix} & * \\ * & \end{pmatrix}$$

of $\mathrm{GL}_2\left(\prod_{\ell\in\Lambda} \mathbb{Z}/\ell\mathbb{Z}\right)$. Thus the image of $\rho\colon G_K \to \mathrm{GL}_2\left(\prod_{\ell\in\Lambda} \mathbb{Z}/\ell\mathbb{Z}\right)$ lies in H. It is a classical fact that $\rho(G_{KF})$ is open in D (see for example, the Corollaire on page 302 of [Ser72]), so $\rho(G_K)$ is open in H. By deleting a few primes from Λ, we may assume that $\rho(G_K)$ contains D, and hence equals D or H, depending on whether $F \subseteq K$ or not.

Let π_ℓ be the probability that a random element of the subgroup $\begin{pmatrix} * & \\ & * \end{pmatrix} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has a nontrivial fixed vector. A calculation shows that $\pi_\ell = 2/\ell + O(1/\ell^2)$. Since Λ has density $1/2$, the series $\sum_{\ell\in\Lambda} 1/\ell$ diverges. Thus $\sum_{\ell\in\Lambda} \pi_\ell$ diverges. Elementary probability shows that if $X_1, X_2, \ldots$ are independent events, and the sum of their probabilities diverges, then as $C \to \infty$, the probability that fewer than t of the first C events occur tends to 0. Therefore as $C \to \infty$, if σ is chosen uniformly at random from the image of D in $\prod_{\ell\in\Lambda,\ell<C} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then the probability that σ has fewer than t components with a nontrivial fixed vector tends to 0.

Similarly, a random element of the coset $\begin{pmatrix} & * \\ * & \end{pmatrix} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has a nontrivial fixed vector with probability $1/\ell + O(1/\ell^2)$. Thus the probability that a random σ from the image of $H - D$ in $\prod_{\ell\in\Lambda,\ell<C} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has fewer than t components with a nontrivial fixed vector tends to 0.

Combining the previous two paragraphs shows that the same holds for a random element of the image I_C of $G_K \to \prod_{\ell\in\Lambda,\ell<C} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. But the Chebotarev Density Theorem implies that the images of the Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$ in I_C are equidistributed in I_C. Finally we apply the "key first step" mentioned at the beginning of this proof to get the desired result. □

Using the preceding lemma, the proof that $\mathcal{T}_2^a$ has follows exactly the proof of Proposition 9.4 in [Poo03], using $\mathbf{N}\mathfrak{p}$ in place of p in the inequalities.

Thus $\mathcal{T}_1$ and $\mathcal{T}_2$ have density 0.

3.8. **Convergence and discreteness.**

Lemma 3.12. *For each $v \in \mathcal{M}_K$, the sequence $\ell_1 P$, $\ell_2 P$, $\ldots$ converges in $E(K_v)$ to P.*

Proof. It suffices to show that $(\ell_i - 1)P \to O$ in $E(K_v)$ as $i \to \infty$. If v is archimedean, this holds by condition (6) in the construction of the ℓ_i. Now suppose v is nonarchimedean. Then the topological group $E(K_v)$ has a basis consisting of open finite-index subgroups U, namely the groups in the filtration appearing in the proof of [Sil92, VII.6.3]. So it suffices to show, given U, that $(\ell_i - 1)P \in U$ for sufficiently large i. Let j be the index of U in $E(K_v)$. If $i \geq j$, then $j \mid i! \mid \ell_i - 1$, by condition (5) in the construction of the ℓ_i, so $(\ell_i - 1)P \in U$. □

Proposition 3.13. *Let $\mathcal{S}$ be as in Lemma 3.9. Let $A := \{x_{\ell_1}, x_{\ell_2}, \dots\}$. Then A is a Diophantine subset of $\mathcal{O}_{K,\mathcal{S}}$. For any $v \in \mathcal{M}_K$, the set A is discrete when viewed as a subset of K_v.*

Proof. By Lemma 3.9, $x(\mathcal{E})$ is the union of the set $A := \{x_{\ell_1}, x_{\ell_2}, \dots\}$ and a finite set. Since $\mathcal{E}$ is Diophantine over $\mathcal{O}_{K,\mathcal{S}}$, so is A.

By Lemma 3.12, the elements of A form a convergent sequence in K_v, and the limit x_1 of the sequence is not in A, so A is discrete. □

This completes the proof of part (1) of Theorem 1.9.

3.9. **A Diophantine model of $\mathbb{Z}$.** We next show how to find a Diophantine model of the ring $\mathbb{Z}$ over certain rings $\mathcal{O}_{K,\mathcal{S}}$.

Lemma 3.14. *Let $B = \{\, 2^n + n^2 : n \in \mathbb{Z}_{\geq 1} \,\}$. Multiplication admits a positive existential definition in the structure $\mathcal{Z} := (\mathbb{Z}_{\geq 1}, 1, +, B)$. (Here B is considered as a unary predicate.)*

Proof. We can define $>$ by

$$x > y \quad \iff \quad (\exists z)\ x = y + z$$

and for fixed $a \in \mathbb{Z}$, we have

$$x \neq a \quad \iff \quad (x > a) \vee (a > x),$$

so this predicate is positive existential in $\mathcal{Z}$. For fixed $c \in \mathbb{Z}_{\geq 1}$, the function $x \mapsto cx$ is positive existential, since it can be obtained by repeated addition.

Call x, y *consecutive* if there exists $n \in \mathbb{Z}_{\geq 1}$ such that $x = 2^n + n^2$ and $y = 2^{n+1} + (n+1)^2$. The set of such (x, y) is positive existential in $\mathcal{Z}$ since it differs from

$$\{\, (x, y) \in B^2 : x < y < 3x \,\}$$

in a finite set. Next

$$\{\, ((2y - z) - (2x - y), 2x - y) : \ x, y \text{ are consecutive and } y, z \text{ are consecutive} \,\}$$

equals the set $T := \{\, (2n - 1, n^2 - 2n - 1) : n \in \mathbb{Z}_{\geq 1} \,\}$. We have

$$(u = v^2) \wedge (v > 0) \quad \iff \quad (2v - 1, u - 2v - 1) \in T.$$

Call this relation $P(u, v)$. Then

$$\begin{aligned} u = v^2 \quad &\iff \quad P(u, v) \vee P(u, -v) \vee ((u = 0) \wedge (v = 0)), \\ u = vw \quad &\iff \quad (v + w)^2 = v^2 + w^2 + 2u, \end{aligned}$$

so we can construct a positive existential definition of multiplication. □

Remark 3.15. Y. Matijasevič (private communication) independently discovered a recursive set B such that multiplication admits a positive existential definition in $(\mathbb{Z}_{\geq 1}, 1, +, B)$.

Corollary 3.16. *The structure $(\mathbb{Z}, 0, 1, +, \cdot)$ admits a positive existential model in the structure $\mathcal{Z}$.*

Because of Corollary 3.16, instead of finding a Diophantine model of the ring $\mathbb{Z}$ over $\mathcal{O}_{K,\mathcal{S}}$, it will suffice to find a Diophantine model of $\mathcal{Z}$.

Now we redo the construction in Section 3.6, but change some of the conditions defining the sequence of primes ℓ_i. Fix $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}_K - \mathcal{S}_{\text{bad}}$ of degree 1 such that neither $\mathfrak{p}$ nor $\mathfrak{q}$ divides $y_1 = y(P)$, and such that the underlying primes $p, q \in \mathcal{P}_{\mathbb{Q}}$ are distinct and odd. Let $M = pq\#E(\mathbb{F}_{\mathfrak{p}})\#E(\mathbb{F}_{\mathfrak{q}})$. Keep conditions (1) through (4), but replace conditions (5) and (6) by the following:

(5′) $\ell_i \equiv 1 \pmod{M}$,
(6′) the highest power of p dividing $(\ell_i - 1)/M$ is p^i, and
(7′) q divides $(\ell_i - 1)/M$ if and only if $i \in B$.

Proposition 3.17. *The sequence $\ell_1, \ell_2, \dots$ is well-defined and computable.*

Proof. The proof is the same as that of Proposition 3.8 except that instead of Lemma 3.6, we will use just Dirichlet's theorem on primes in arithmetic progressions to show that conditions (5′) through (7′) are satisfied by a positive density of primes ℓ_i.

The conditions amount to congruences modulo $p^{i+1}qM$, so it suffices to show that one of the congruence classes is of the form $a \pmod{p^{i+1}qM}$ with $(a, p^{i+1}qM) = 1$. Define

$$a = \begin{cases} 1 + p^i qM & \text{if } i \in B \\ 1 + (p^i q + p^{i+1})M & \text{if } i \notin B. \end{cases}$$

Then a is congruent to 1 modulo p, modulo q, and modulo M, so $(a, p^{i+1}qM) = 1$. Any prime in the residue class $a \pmod{p^{i+1}qM}$ satisfies (5′) through (7′). □

Lemma 3.18. *If $m \in \mathbb{Z}_{\geq 1}$, then*

$$\operatorname{ord}_{\mathfrak{p}}(x_{mM+1} - x_1) = \operatorname{ord}_{\mathfrak{p}}(x_{M+1} - x_1) + \operatorname{ord}_p m.$$

Proof. Let R be the valuation ring $R_{\mathfrak{p}}$ defined in Section 3.1. Because $y_1 \in R^*$ and $\mathfrak{p} \nmid 2$, for any $r \geq 1$, the restriction of the x-coordinate map $E(R/\mathfrak{p}^r) \to \mathbb{P}^1(R/\mathfrak{p}^r)$ to the subset of points of $E(R/\mathfrak{p}^r)$ with the same image in $E(R/\mathfrak{p})$ as P is injective (the y-coordinate can be recovered from the the x-coordinate as the square root of an element of R^*: its sign is determined by the fact that the point is in the residue class of P). Thus for $r \geq 1$, the ideal $\mathfrak{p}^r$ divides $x_{mM+1} - x_1$ if and only if $(mM + 1)P$ and P have the same image in $E(R/\mathfrak{p}^r)$, or equivalently if $(mM)P$ maps to O in $E(R/\mathfrak{p}^r)$. Let $z \in \hat{E}(\mathfrak{p}R)$ be the point of the formal group corresponding to MP. Then the condition that $(mM)P$ maps to O in $E(R/\mathfrak{p}^r)$ is equivalent to $[m](z) \in \mathfrak{p}^r$, where $[m]$ denotes the multiplication-by-m map in the formal group.

It remains to prove that $\operatorname{ord}_{\mathfrak{p}}[m](z) = \operatorname{ord}_{\mathfrak{p}} z + \operatorname{ord}_p m$. By induction on m, it suffices to prove this when m is prime. Then, in the proof of Lemma 3.3, we have $[m](z) = mf(z) + g(z^m)$ where $f(T), g(T) \in R[[T]]$ satisfy $g(0) = 0$ and $f(T) = T +$higher order terms. Finally $\operatorname{ord}_{\mathfrak{p}} m = \operatorname{ord}_p m$ is 1 or 0 according to whether $m = p$ or not, so the result follows. □

Proposition 3.19. *Let $\mathcal{S}$ be as in Lemma 3.9. Let $A := \{x_{\ell_1}, x_{\ell_2}, \dots\}$. Then A is a Diophantine model of $\mathcal{Z}$ over $\mathcal{O}_{K,\mathcal{S}}$, via the bijection $\phi \colon \mathbb{Z}_{\geq 1} \to A$ taking i to x_{ℓ_i}.*

Proof. The set A is Diophantine over $\mathcal{O}_{K,\mathcal{S}}$ by the argument in the proof of Proposition 3.13.

We have

$$\begin{aligned} i \in B \quad &\iff \quad q \text{ divides } (\ell_i - 1)/M && \text{(by condition (7'))} \\ &\iff \quad \operatorname{ord}_{\mathfrak{q}}(x_{\ell_i} - x_1) > \operatorname{ord}_{\mathfrak{q}}(x_{M+1} - x_1), \end{aligned}$$

by Lemma 3.18 (with $\mathfrak{q}$ in place of $\mathfrak{p}$). The latter inequality is a Diophantine condition on x_{ℓ_i}, by Corollary 2.3 (in which we represent elements of K as ratios of elements of $\mathcal{O}_{K,\mathcal{S}}$). Thus the subset $\phi(B)$ of A is Diophantine over $\mathcal{O}_{K,\mathcal{S}}$.

Finally, for $i \in \mathbb{Z}_{\geq 1}$, Lemma 3.18 and condition (6') imply $\operatorname{ord}_{\mathfrak{p}}(x_{\ell_i} - x_1) = c + i$, where the integer $c = \operatorname{ord}_{\mathfrak{p}}(x_{M+1} - x_1)$ is independent of i. Therefore, for $i, j, k \in \mathbb{Z}_{\geq 1}$, we have

$$i + j = k \quad \iff \quad \operatorname{ord}_{\mathfrak{p}}(x_{\ell_i} - x_1) + \operatorname{ord}_{\mathfrak{p}}(x_{\ell_j} - x_1) = \operatorname{ord}_{\mathfrak{p}}(x_{\ell_k} - x_1) + c.$$

It follows that the graph of + corresponds under ϕ to a subset of A^3 that is Diophantine over $\mathcal{O}_{K,\mathcal{S}}$.

Thus A is a Diophantine model of $\mathcal{Z}$ over $\mathcal{O}_{K,\mathcal{S}}$. □

As already remarked, Corollary 3.16 and Proposition 3.19 together imply part (2) of Theorem 1.9.

Acknowledgements

We thank Ernie Croot for a discussion regarding Lemma 3.6.

References

[CF86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[CTSSD97] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Peter Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135.

[CZ00] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 253–260.

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Springer-Verlag, New York, 1994.

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.

[Maz94] Barry Mazur, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371.

[Maz95] Barry Mazur, *Speculations about the topology of rational points: an update*, Astérisque (1995), no. 228, 4, 165–182, Columbia University Number Theory Seminar (New York, 1992).

[Maz98] B. Mazur, *Open problems regarding rational points on curves and varieties*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 239–265.

[Mon94] Hugh L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[Phe94] Thanases Pheidas, *Extensions of Hilbert's tenth problem*, J. Symbolic Logic **59** (1994), no. 2, 372–397.

[Poo03] Bjorn Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$, J. Amer. Math. Soc. **16** (2003), no. 4, 981–990.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shl] Alexandra Shlapentokh, *On diophantine definability and decidability in some infinite totally real extensions of* $\mathbb{Q}$, to appear in Trans. Amer. Math. Soc.

[Shl94] Alexandra Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), no. 1, 139–175.

[Shl97] Alexandra Shlapentokh, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, Invent. Math. **129** (1997), no. 3, 489–507.

[Shl00a] Alexandra Shlapentokh, *Defining integrality at prime sets of high density in number fields*, Duke Math. J. **101** (2000), no. 1, 117–134.

[Shl00b] Alexandra Shlapentokh, *Hilbert's tenth problem over number fields, a survey*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 107–137.

[Shl02] Alexandra Shlapentokh, *Diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2*, J. Number Theory **95** (2002), no. 2, 227–252.

[Shl03] Alexandra Shlapentokh, *A ring version of Mazur's conjecture on topology of rational points*, Internat. Math. Res. Notices (2003), no. 7, 411–422.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[Wey16] Hermann Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1916), 313–352.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu
URL: http://math.berkeley.edu/~poonen

Department of Mathematics, East Carolina University, Greenville, NC 27858, USA
E-mail address: shlapentokha@mail.ecu.edu
URL: http://www.personal.ecu.edu/shlapentokha